一种轻量级的雾计算属性基外包加密算法 *

曾 萍[1]，钱 进[1, 2]，穆成新[3]，高 原[1]，胡荣磊[1]

(1. 北京电子科技学院，北京 100000; 2. 西安电子科技大学 通信工程学院，西安 710000; 3. 空军哈尔滨飞行学院理论训练系，哈尔滨 150001)

摘 要：基于属性的加密算法拥有灵活、细粒度、安全性高等特点，为减少属性基加密算法占用的资源，在安全数据访问控制的属性基加密算法的基础上提出了一种改进的属性基外包加密算法。改进算法将加密算法中的复杂双线性对计算外包给雾节点以减少用户的计算开销；同时通过简化系统参数，减少属性中心为属性生成的随机因子以缩短密文和密钥长度，降低了用户和雾节点的存储和通信开销。同时对提出的改进算法进行了安全性证明，证明了该改进算法是安全的。

关键词：属性基加密；加密外包；雾计算；安全性证明；门限分割

中图分类号：TP309.7 doi: 10.19734/j.issn.1001-3695.2018.06.0556

Light weight attribute-based encryption outsourced algorithm for fog computing

Zeng Ping[1], Qian Jin[1, 2], Mu Chenxin[3], Gao Yuan[1], Hu Ronglei[1]

(1. *Beijing Electronics Science & Technology Institute*, *Beijing* 100000, *China*; 2. *School of Communication & Engineering*, *Xidian University*, *Xi'an* 710000, *China*; 3. *Dept. of Theoretical Training*, *People's Liberation Army Air Force Harbin Flight Academy*, *Harbin* 150001, *China*)

Abstract: Attribute-based encryption algorithm has the characteristics as flexibility, fine-grained and high security. This paper introduces an improved attribute-based outsourced encryption algorithm based on secure data access control attribute-based encryption, to reduce the resources consumed by computation, which outsources the complex bilinear pairings in the encryption computing to the fog node to reduce the user's computation overhead. By simplifying the system parameters, we reduce the random number generated by attribute authority for every attribute to shorten the length of ciphertext and the key, as well as the storage cost of the system. And the security proof of the scheme is given in the last part of this paper.

Key words: attribute-based encryption; outsourcing encryption; fog computing; security analysis; threshold segmentation

0 引言

云计算是一种基于共享建立的新计算模式，用户将需要托管和分析的数据传输到云平台进行管理[1]。而雾计算作为对云计算的拓展，将计算迁移到靠近用户端的雾计算节点，有效节省了云平台的网络开销，避免了云平台的网络性能瓶颈[2]。但是这样会带来雾计算设备管理问题，雾计算节点由于部署在云平台的远端缺乏持续有效的管理，极易受到攻击；用户设备与雾节点之间缺乏有效的信任机制，此外雾节点还要接受来自多种异构设备的访问，大量的用户设备接入网络使得用户管理变得异常困难[3]。

密文策略的属性基加密方案(ciphertext-policy attribute-based encryption)通过对密文标定属性，规定访问者的访问策略，实现用户对数据的细粒度访问。虽然这种方案克服了用户访问过程中的粒度控制问题，但同时也带来了属性管理的问题。密钥生成中心根据用户的属性集生成相应的私钥，但如何隐藏私钥中带有用户属性集的特征，保证属性集信息不被泄露是一个问题。此外当用户更新、添加或是撤销属性时，密钥生成中心需要根据新的属性集更新密钥。如何保证改变的属性不被暴露，撤销的属性被彻底销毁以及如何保证密钥更新的前后向安全性都是目前急需解决的困难的问题。属性基加密方案最先在文献[4]中提出。为了克服该方案中访问不灵活的缺点，文献[5]中提出了密文策略的加密方案，将属性关联于密文，接收方根据密文规定的属性集判断自己能否进行解密。基于属性的签名(ABS)方案[6]可以实现认证功能，但是不能实现安全通信。文献[7]在标准模型下证明了文献[6]中签名算法的安全性，但是不能应用于雾计算加解密外包的环境。文献[8]改进了签名算法使其可以运用于加解密外包环境下，但是不能保证数据的安全性。文献[9]提出了一种由分层的身份基加密方案演变而来的属性基加密方案，方案中使用了混合双系统加密，方案的灵活性大大加强，用户可以指定任意深度的访问策略，但是方案涉及多个乘法群上的双线性变换，计算量过大。文献[10]提出了一种属性与角色混合加密算法，兼有细粒度和访问灵活的特点，但是安全性有所下降。文献[11]提出了一种带有属性更新功能的外包加密方案。文献[12]提出了一种改进的属性基加密方案，通过减少乘法循环群上的计算次数来减少用户的计算开销，同时能够按照用户属性集的变化进行密文更新。文献[13]提出一种安全性更高的属性基加密方案，但是由于该方案为多认证中心方案，认证交互次数过多，不适合雾计算环境。文献[14]提

收稿日期：2018-06-20；**修回日期：**2018-09-10 **基金项目：**国家自然科学基金青年基金资助项目（61201159）；国家自然科学基金面上项目（61772047）

作者简介：曾萍（1969-），女，广东潮安人，教授，博士，主要研究方向为网络安全（zengping69@sina.com）；钱进（1993-），男，江苏扬州人，硕士研究生，主要研究方向为物联网安全；穆成新（1976-），男，黑龙江哈尔滨人，讲师，学士，主要研究方向为飞行通信与领航；高原（1979-），女，辽宁沈阳人，讲师，博士，主要研究方向为网络安全；胡荣磊，男，河北景县人，副教授，博士，主要研究方向为信息安全.

出了一种适用于雾计算环境的加密方案，但由于该方案使用多认证中心，使得用户的通信开销过大，因此不适宜运用在移动设备上。

本文主要工作为设计一种改进的适用于雾计算的属性基加密算法，简化系统参数，减少属性中心为属性生成的随机因子以缩短密文和密钥长度，降低了用户和雾节点的存储和通信开销。同时利用标准模型对提出的改进算法进行了安全性证明，证明了该改进算法是安全的。

1　技术基础

a）双线性变换[15]为一种在乘法群上的映射。设有一大素数 q，定义 G_0 和 G_1 为两个阶为 q 的乘法循环群，运行在群 G_0 上的映射 $e:G_0\times G_0\to G_1$ 满足以下三种性质时被称做双线性映射：

(a)双线性。对于任意的群 G_0 上的元素 $g,p,r\in G_0$ 和 $a,b\in Z_q$ 都有 $e(g^a,p^b)=e(g,p)^{ab}$ 和 $e(gp,r)=e(g,r)\cdot e(p,r)$。

(b)非退化性。当 g 是 G_0 时，$e(g,g)$ 是 G_1 的单位元，且 e 不把 G_0 的所有元素对都映射到 G_1 的单位元。

(c)可计算性。对于任意 $g,p\in G$ 都有有效的算法计算 $e(g,p)$。

b)判定性双线性问题(DBDH)。假设存在 q 阶循环群 G_0 和群上的元素 p 以及运行在群上的双线性变换 e，随机选定整数 $a,b,c\in Z_q$，给定两个元组 $(p,p^a,p^b,p^c,e(p,p)^{abc})$ 和 (p,p^a,p^b,p^c,k) 其中 k 是和 $e(p,p)^{abc}$ 同分布的随机比特串，区分两个元组中哪一个是随机元组。

2　安全模型

本文采用标准模型证明加密方案的安全性。模型中假设云平台是安全的，利用挑战者和攻击者之间的博弈游戏描述模型，具体过程如下：

系统初始化：向系统 $\mathcal{S}$ 输入公共参数 $params$。

查询阶段 1：攻击者 $\mathcal{A}$ 可以向系统提出任意属性集，系统运行 $KeyGen$ 算法生成相应的私钥 SK 并返回给攻击者。

挑战阶段：攻击者向系统提供两个等长的明文 m_0 和 m_1，并向系统提出一个访问结构 T_a，该结构不能在查询阶段 1 被查询过且不能是询问阶段任何结构的子树。系统随机选取一个比特 $b\in\{0,1\}$，并生成结构 T_a 的私钥，对明文 m_b 进行加密得到密文 C_b 并返回给攻击者。

查询阶段 2：攻击者继续向系统提出询问，该阶段不能进行对结构 T_a 和以 T_a 为子树的询问。系统继续向攻击者提供查询信息。

猜测阶段：攻击者根据查询结果猜测挑战阶段获得的密文是 m_0 和 m_1 中哪一个的密文，攻击者输出相应的比特 $b'\in\{0,1\}$，攻击者的优势定义为 $Adv=|\Pr[b=b']-1/2|$。

3　加密方案设计

3.1　系统简介

如图 1 所示。本系统包含四个部分，即云平台、雾节点、数据拥有者和其他访问用户。云平台负责生成系统参数，决定系统的安全等级、承担属性中心的工作，同时还要调度雾计算节点的资源以及处理用户的接入认证请求，生成用户的密钥。雾节点负责与用户进行通信，传递用户的认证信息，代替用户完成数据的加密外包工作，确保数据只能被符合一定属性要求的用户进行解密。数据拥有者利用自己的私钥对明文进行用户加密，确保密文不会被非法用户解密。当访问用户提出数据访问请求时，首先检查密文是否可以被正确解密，若可以被正确解密，即指定雾节点进行外包解密，访问用户在收到雾节点的部分解密密文后进行用户解密，得到明文。

3.2　设计思想

为简化加密的复杂度并节省开销，可以将加解密计算外包给加雾节点。在保证安全性的前提下，为进一步简化外包给雾节点的加密解过程，通过减少雾节点加入到部分密文中的随机因子，可以将原有密文长度缩短一半。同时由雾节点指定部分密文中的秘密分量，保证了前向安全性。

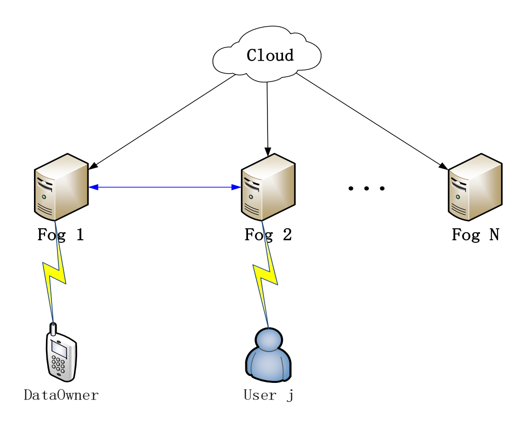


图 1　系统架构图

Fig. 1　System architecture diagram

加密方案的设计流程如下：

a) $SysSetup(k)$：属性中心输入安全参数 k，产生系统参数 $params$。算法生成 q 阶乘法群 G_0 和 G_1，其中 q 为一个大素数，同时生成双线性映射 $e:G_0\times G_0\to G_1$ 和哈希函数 $H:\{0,1\}^*\to G_0$。属性中心选取随机数 $\alpha,\beta\in Z_q$，计算云平台公钥 $PK_c=g^\alpha$，云平台主密钥为 $MSK_c=\alpha$。系统参数为 $params=(g,h,g^\alpha,e,e(h,g),H)$。

b) $AttrSetup(params,A)$：属性中心获取系统参数后为每一个属性生成密钥分量，其中 A 为属性集。假设 A 中有 N 个属性，则 A 可以表示为 $\{attr_1,attr_2,\ldots,attr_N\}$，其中的 $attr_i$ 为某一属性，将所有属性看做是互不相同的比特串，对于所有属性计算 $\lambda_1=H(attr_1)$，$\lambda_2=H(attr_2)\ldots\lambda_N=H(attr_N)$。计算，$D_1=\lambda_1^{\alpha}$，$D_2=\lambda_2^{\alpha}\ldots D_N=\lambda_N^{\alpha}$。

c) $KeyGen(params,A_i)$：属性中心输入某一用户 U_i 的属性集 A_i 和系统参数 $params$，生成对应的密钥。假设属性集 A_i 为 $\{Ua_1,Ua_2,\ldots,Ua_n\}$，其中 Ua_i 为用户拥有的属性。属性中心为用户选取唯一的随机数 $\omega\in Z_q$，计算用户密钥 $SK=g^{\alpha(\beta+\omega)}$ 和外包密钥 $SK'=\{g^{\omega}h^{\varepsilon},g^{\varepsilon},C_0=PK^{\omega},C_j=D_j^{\omega}\}_{j\in A_i}$。

d) $FogEncrypt(SK',T_U)$：雾节点收到加密外包密钥 SK' 和用户的属性策略 T_U 后选取随机数 $m\in Z_q$。雾节点将 m 作为分割秘密数，根据用户的属性策略利用门线分割方法计算 m 分割后的分量 $\{y_1(0),y_2(0),\ldots,y_n(0)\}$ 并计算 $CT'=\{g^{y_1(0)}D_1,g^{y_2(0)}D_2,\ldots,g^{y_n(0)}D_n\}$ 和 $T=g^{\alpha m},h^{\alpha m}$。

e) $UserEncrypt(C_0,CT',T)$：用户获得 C_0，CT' 和 T 之后进行用户加密，选取随机数 $t,DK\in Z_q$，计算 $T_0=g^{\alpha m}\cdot g^{\alpha t}$，$T_1=h^{\alpha m}\cdot h^{\alpha t}$，$g^t$ 和 $DK\cdot e(g,g)^{\alpha\beta t}$，利用 DK 对明文进行对称加密。密文为 $CT=\{T_0,T_1,g^t,DK\cdot e(g,g)^{\alpha\beta t},CT',SE_{DK}(M)\}$。

f) $FogDecrypt$：雾节点 2 接收到 CT 后进行外包解密。雾节点

点 2 利用用户的外包密钥 $SK'=\{g^{\omega}h^{\varepsilon},g^{\varepsilon},C_0=PK^{\omega},C_j=D_j^{\omega}\}_{j\in A_i}$ 计算

$$F_j=\frac{e\left(g^{y_j(0)}D_j,C_0'\right)}{e\left(PK,C_j'\right)}=e(g,g)^{y_j(0)\alpha\omega} \tag{1}$$

从访问结构的叶子节点开始计算父节点的值：

$$\begin{aligned}F&=\prod_{x\in children}\left(e(g,g)^{y_{parent}(index(x))\alpha\omega}\right)^{p_{parent}(0)}\\&=\prod_{x\in children}e(g,g)^{y_x(0)\alpha\omega p_x(0)}\\&=e(g,g)^{y_{parent}(0)\alpha\omega}\end{aligned} \tag{2}$$

依此类推可以还原出 $e(g,g)^{m\alpha\omega'}$。同时计算

$$\frac{e\left(g^{\omega}h^{\varepsilon},g^{\alpha(m+t)}\right)}{e\left(g^{\varepsilon},h^{\alpha(m+t)}\right)}=e(g,g)^{\alpha\omega(m+t)} \tag{3}$$

$$\frac{e(g,g)^{\alpha\omega(m+t)}}{e(g,g)^{\alpha\omega m}}=e(g,g)^{\alpha\omega t} \tag{4}$$

g) *UserDecrypt*：用户计算对称密钥

$$DK=\frac{DK\cdot e(g,g)^{\alpha\beta t}\cdot e(g,g)^{\alpha\omega t}}{e\left(g^{t},g^{\alpha(\beta+\omega)}\right)} \tag{5}$$

最后解密密文 $Dec(DK,SE_{DK}(M))$ 得到明文。

以上加解密过程如图 2 和 3 所示。

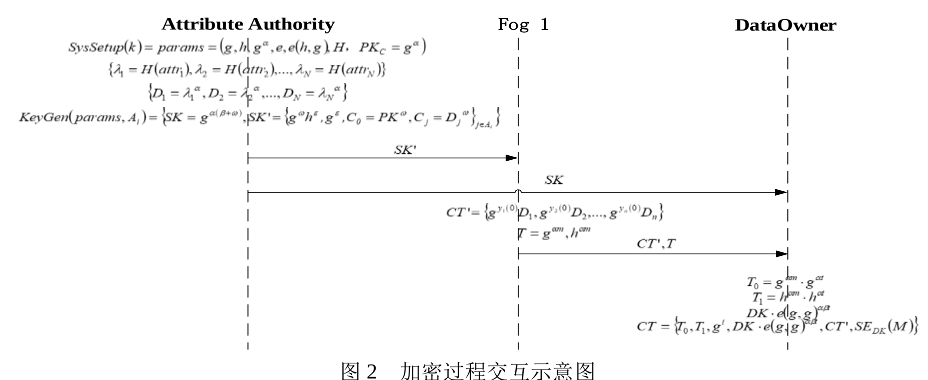


图 2　加密过程交互示意图

Fig. 2　Schematic diagram of encryption process

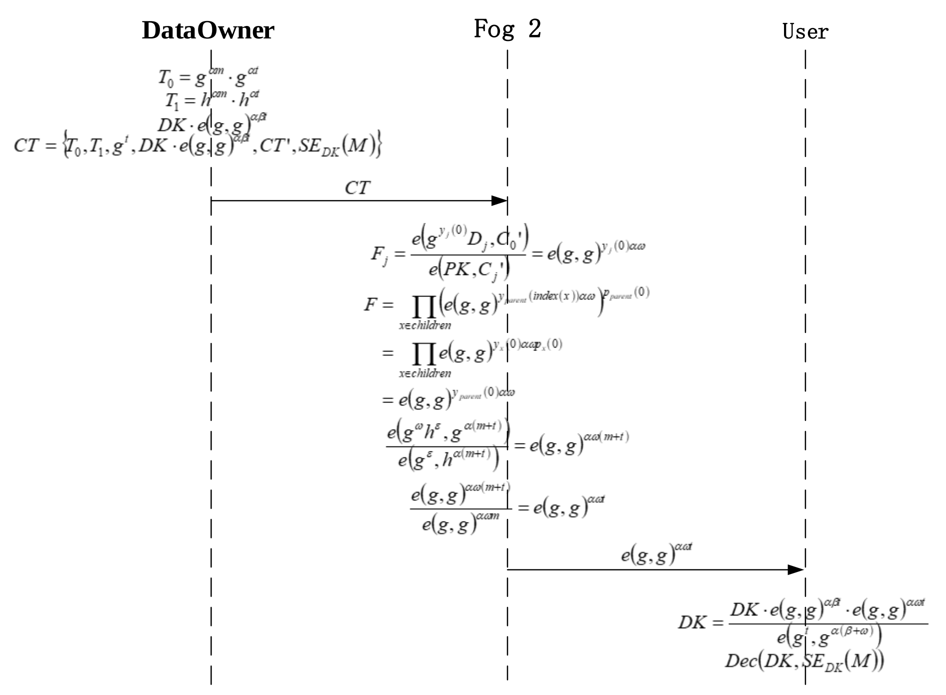


图 3　解密过程交互示意图

Fig. 3　Schematic diagram of decryption process

4　安全性证明

假设有一个攻击者 $\mathcal{A}$ 能够以不可忽略的优势 ε 来攻破该系统，那么就存在一个算法 $\mathcal{B}$ 可以调用 $\mathcal{A}$ 来解决 DBDH 问题。假设系统一共有 k_N 个属性结构。

初始化： 系统生成 q 阶群 G_0,G_1 和双线性映射 $e:G_0\times G_0\to G_1$，选取生成元 $g,h\in G_0$ 和随机数 $\alpha\in Z_q$ 以及属性集 $A=\{attr_1,attr_2,...,attr_N\}$ 共 N 个属性，其中 $N\le q$，计算 $D_1=H(attr_1)^{\alpha}$，$D_2=H(attr_2)^{\alpha}$，$D_N=H(attr_N)^{\alpha}$。挑战者 $\mathcal{B}$ 选定自己要解决的 DBDH 问题 $(A=g^a,B=g^b,C=g^c,D=g^{abc})$，同时从 A 中选取子集作为 *Corrupted* 属性集 $A_b=\{a_1,a_2,...,a_M\}$，其中 a_i 为某一属性，A_b 中有 M 个属性。挑战者计算 $B_1=H(a_1)^a$，$B_2=H(a_2)^a$，$B_M=H(a_M)^a$。

询问阶段 1: 攻击者 $\mathcal{A}$ 向挑战者 $\mathcal{B}$ 询问一个属性结构 T_a，结构的属性集为 $A_a=\{attr_1,attr_2,...,attr_m\}$。挑战者建立一张表 *Table* 记录属性结构 T_a 以及相应的私钥 SK，该表对 $\mathcal{B}$ 是完全透明的，$\mathcal{B}$ 可以随时查询该表。挑战者根据攻击者的询问内容分情况进行处理：

情况 1　如果 $A_a\cap A_b=\varnothing$，挑战者选取随机数 $\omega,\varepsilon\in Z_q$，

计算密钥 $SK = g^{\alpha(\beta+\omega)}$ 和 $SK' = \{g^{\omega}h^{\varepsilon}, g^{\varepsilon}, C_0 = PK^{\omega}, C_j = D_j^{\omega}\}_{j\in A_a}$，将密钥发送给攻击者。挑战者输出随机比特 $b \in \{0,1\}$ 并停止攻击。

情况 2　如果 $A_a \cap A_b \neq \varnothing$ 且 $A_a \not\subset A_b$，挑战者选取随机数 $\omega, \varepsilon \in Z_q$，计算密钥 $SK = g^{\alpha(\beta+\omega)}$ 和 $SK' = \{g^{\omega}h^{\varepsilon}, g^{\varepsilon}, C_0 = PK^{\omega}, C_j = D_j^{\omega}\}_{j\in A_a}$，将密钥发送给攻击者。挑战者输出随机比特 $b \in \{0,1\}$ 并停止攻击。

情况 3　如果 $A_a \subset A_b$，挑战者选取随机数 $\omega, \varepsilon \in Z_q$，计算密钥 $SK = g^{a(b+\omega)}$，$C_0 = g^{a\omega}$ 和 $\{C_j = B_j^{\omega}\}_{j\in A_a}$，外包密钥为 $SK' = \{g^{\omega}h^{\varepsilon}, g^{\varepsilon}, C_0, \{C_j\}_{j\in A_a}\}$ 将密钥发送给攻击者，同时将 SK，SK' 和 T_a 记入表中。

假设该阶段进行了 q_{E1} 次询问。

挑战阶段：攻击者生成两个等长明文 m_0 和 m_1 以及想挑战的属性结构 T_A 给挑战者。挑战者计算 $D_1 = \lambda_1^{a}, D_2 = \lambda_2^{a}, \ldots, D_N = \lambda_N^{a}$ 同时为 T_A 选取随机数 $\omega, \varepsilon \in Z_q$，生成密钥 $SK = g^{a(b+\omega)}$ 和 $SK' = \{g^{\omega}h^{\varepsilon}, g^{\varepsilon}, C_0 = PK^{\omega}, C_j = D_j^{\omega}\}_{j\in A_a}$。挑战者选取随机比特 $v \in \{0,1\}$，用该密钥加密明文 m_v。将常数 b 作为秘密分割数得到 $\{y_1(0), y_2(0), \ldots, y_m(0)\}$，计算 $T_0 = g^{a(m+c)}$ 和 $T_1 = h^{a(m+c)}$，部分密文为密文 $CT' = \{g^{y_1(0)}D_1, g^{y_2(0)}D_2, \ldots, g^{y_n(0)}D_n\}$。设置 $t = c$ 完全密文为 $CT = \{T_0, T_1, g^{t}, DK \cdot e(g,g)^{\alpha\beta t}, CT', SE_{DK}(M)\}$ 因为：

$$\frac{e\left(g^{y_i(0)}\lambda_i^{\alpha}, g^{\alpha\omega'}\right)}{e\left(g^{\alpha}, \lambda_i^{\alpha\omega'}\right)} = e\left(g^{y_i(0)}, g^{\alpha\omega'}\right) \tag{6}$$

$$\begin{aligned} F_{Root} &= \prod_{x\in children} F_x^{\Delta_{index(x),S'_x}(0)} \\ &= \prod_{x\in children} e(g,g)^{\alpha\omega q_{parent(x)}(index(x))\Delta_{index(x),S'_x}(0)} \\ &= e(g,g)^{\alpha\omega \sum_{x\in children} q_{parent(x)}(index(x))\Delta_{index(x),S'_x}(0)} \\ &= e(g,g)^{\alpha\omega q_{Root}(0)} \end{aligned} \tag{7}$$

且 $e(g,g)^{\alpha\beta t} = e(g,g)^{abc}$，所以 $DK \cdot e(g,g)^{\alpha\beta t}$ 是有效密文。

询问阶段 2：攻击者继续选取询问结构向挑战者进行询问，挑战者查表，询问的结构不能是表中任一结构的子树，假设该阶段询问了 q_{E2} 次。

猜测阶段：攻击者根据查询的结果猜测密文对应于哪一个明文，输出比特 $b' \in \{0,1\}$。

证明：要使攻击者能够顺利进行攻击就需要攻击者能够正确地进行询问，询问阶段 1 的属性必须包含于属性集 A_b。系统共有 N 个属性，而挑战者掌握的已 *Corrupted* 的属性有 M 个，挑战者可以利用这些属性将 DBDH 问题嵌入到这些属性中，前提是攻击者提出的属性不能超出 A_b。从 N 个属性中任意选取属性共有 2^N 种选择，正确的情况有 2^M 种。所有询问都正确的概率是 $2^{(M-N)(q_{E1}+q_{E2})}$，因为 $|\Pr[b = b'] - 1/2| = \varepsilon$，所以：

$$\begin{aligned} &\Pr\left[f\left(g^a, g^b, g^c, e(g,g)^{abc}\right) - f\left(g^a, g^b, g^c, K\right) \neq 0\right] \\ &\geq \Pr[\exists A_a : A_a - A_b \neq \varnothing] \times 1/2 + \Pr[\forall A_a : A_a \subset A_b] \times (1/2 - \varepsilon) \\ &= \left(1 - 2^{(M-N)(q_{E1}+q_{E2})}\right) \times 1/2 + 2^{(M-N)(q_{E1}+q_{E2})} \times (1/2 - \varepsilon) \\ &= 1/2 - 2^{(M-N)(q_{E1}+q_{E2})}/2 + 2^{(M-N)(q_{E1}+q_{E2})}/2 - 2^{(M-N)(q_{E1}+q_{E2})} \times \varepsilon \\ &= 1/2 - 2^{(M-N)(q_{E1}+q_{E2})} \times \varepsilon \end{aligned} \tag{8}$$

其中 ε 不大于 1/2，所以$\mathcal{B}$的优势不大于 $2^{(M-N)(q_{E1}+q_{E2}+1)}$。证毕。

5　性能比较

将本文的方案与文献[11，12]的方案进行比较，比较的标准分为时间和空间两个指标。首先对所有方案进行时间指标的分析，为隐藏用户的属性信息需要对每个属性进行隐藏，相应地需要对每个属性进行双线性变换，本文的方案与文献[12]在解密时计算量相近。由于运用了外包加密算法，大部分的加解密计算不需要用户来完成。

表 1　加密计算量比较

Table 1　Comparison of cost of encrytion

scheme	outsourcing encrypt	encrypt of user
Scheme in [11]	(|S|+2)C	5C+2C$_T$
Scheme in [12]	(2|S|+2)C	2C+2C$_T$
本文方案	(|S|+2)C	3C+2C$_T$

表 2　解密计算量比较

Table 2　Comparison of cost of decrytion

scheme	outsourcing decrypt	decrypt of user
Scheme in [11]	(2|S|+2)E+(T$_a$+2)C$_T$	(2|S|+1)E+2|S|C$_T$
Scheme in [12]	(2|S|+2)E+(T$_a$+1)C$_T$	E+2C$_T$
本文方案	(2|S|+2)E+(T$_a$+2)C$_T$	E+2C$_T$

文献[12]的方案中的密钥长度为属性数的两倍，因为该算法中需要为每个属性计算单独的双线性变换，变换中的两个因子都不一样，所以该方案中的密钥和密文长度都随着属性的增加而呈现两倍的增长。本文方案的双线性变换会共享一个因子，所以可以节省一半的存储孔家。表中的 S 为用户的属性集，|S|表示 S 内元素个数。|g|是集合 G_0 中的生成元 g 的长度，|g_T|是集合 G_T 的生成元的长度。C 和 C_T 分别表示群 G_0 和 G_1 上的计算，E 表示双线性变换计算。可以看出在保持计算量和安全性不变的基础上大大缩短了密文和密钥的长度，使密文和密钥缩短到原来的一半。

表 3　存储开销比较

Table 3　Comparison of storage

scheme	length of plaintext	length of key
Scheme in [11]	(3|S|+1)|g|+|g$_T$|	(|S|+2)|g|
Scheme in [12]	(2|S|+3)|g|+|g$_T$|	(2|S|+3)|g|
本文方案	(|S|+3)|g|+|g$_T$|	(|S|+3)|g|

6　结束语

本文通过对现有的密文策略属性加密方案进行改进，简化了数据拥有者外包私钥的生成过程，减少了属性中心生成的属性分量的个数，从而缩短了密文和密钥长度，节省了加解密的存储和计算开销，在此基础上保证了系统的安全性不变。本文基于 DBDH 问题在标准模型下证明了该方案的安全性，通过性能分析和安全性证明表明了本文所提方案不但具有较高的效率还有较好的安全性。

参考文献：

[1] 崔勇，宋健，缪葱葱，等. 移动云计算研究进展与趋势 [J]. 计算机学报, 2017, 40(2): 273-295. (Cui Yong, Song Jian, Miao Congcong, *et al*. Research progress and trend of mobile cloud computing [J]. Journal of Computer Science, 2017, 40(2): 273-295.)

[2] 方巍. 从云计算到雾计算的范式转变 [J]. 南京信息工程大学学报, 2016, 8(5): 404-414. (Fang Wei. Paradigm shift from cloud computing to fog computing [J]. Journal of Nanjing University of Information Science and Technology, 2016, 8(5): 404-414.)

[3] Barrett D, Kipper G. Cloud Computing and the Forensic Challenges [J].

Virtualization and Forensics, 2010 (1): 197-209.

[4] Pirretti M, Traynor P, McDaniel P, *et al.* Secure attribute-based systems [J]// Journal of Computer Security, 2010, 18 (5): 799-837.

[5] Bethencourt J, Sahai A, Waters Brent. Ciphertext-Policy attribute-based encryption [C]// Proc of the 29th IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 2007: 321-334.

[6] Maji H K, Prabhakaran M, Rosulek M. Attribute-based signatures [C]// Proc of the 11th International Conference on Topics in Cryptology. Berlin: Springer-Verlag, 2011: 376-392.

[7] Alex Escala, Javier Herranz, Paz Morillo. Revocable attribute-based signatures with adaptive security in the standard model [C]// Proc of the 4th International Conference on Progress in Cryptology in Africa. Berlin: Springer-Verlag, 2011: 224-241.

[8] Li Jin, Chen Xiaofen, Li Jingwei, *et al.* Secure outsourced attribute-based signatures [J]. IEEE Trans on Parallel & Distributed Systems, 2014, 25 (12): 3285-3294.

[9] Lewko A, Waters B. Unbounded HIBE and attribute-based encryption [C]// Proc of the 30th International Conference on Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2011: 547-567.

[10] Jin Xin, Krishnan R, Sandhu R. A unified attribute-based access control model covering DAC, MAC and RBAC [C]// Proc of the 26th of Data and Applications Security and Privacy. Berlin: Springer, 2012: 41-55.

[11] Zhang Peng, Chen Zehong, Joseph K. Liu, *et al.* An efficient access control scheme with outsourcing capability and attribute update for fog computing [J]. Future Generation Computer Systems, 2018(78): 753-762.

[12] Huang Qinlong, Yang Yixian, Wang Licheng. Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of things [J]. IEEE Access, 2017, 5 (99): 12941-12950.

[13] Chase M, Chow S S M. Improving privacy and security in multi-authority attribute-based encryption [C]// Proc of the 16th ACM Conference on Computer and Communications Security. New York: ACM Press, 2009: 121-130.

[14] Li Fei, Yogachandran Rahulamathavan, Muttukrishnan Rajarajan, *et al.* Low complexity multi-authority attribute based encryption scheme for mobile cloud computing [C]// Proc of the 7th IEEE International Symposium on Service-Oriented System Engineering. Piscataway: IEEE Press, 2013: 573-577.

[15] Dan B, Franklin M. Identity-based encryption from the weil pairing [J]. Grypto, 2003, 32(3): 213-229.